Fuite des données et gestion des incidents

EJZYN, Alain; Van Den Berghe, Thierry; Van Gyseghem, Jean-Marc

Published in:
DPO news

Publication date:
2018

Document Version
le PDF de l'éditeur

Dossier

Fuite des données et gestion des incidents

L'impact d'un incident de sécurité peut être mieux maîtrisé quand les acteurs de la sécurité, dont le DPO, ont anticipé un plan réponse préalable pour réagir en bon ordre. Si l'incident entraîne une fuite de données, alors le GDPR prévoit de documenter et de notifier la fuite.

Les trois niveaux d'intervention du DPO

Le GDPR a, entre autres, intégré l'obligation de notifier toute violation de données à caractère personnel[1], mais également un nouvel acteur au côté des responsables et sous-traitants en la personne du DPO.

Le DPO a comme fonction, entre autres, de conseiller les responsables de traitement et sous-traitants, mais également de « faire office de point de contact pour l'[Autorité de Protection des données] sur les questions relatives au traitement »[2]. Ces deux fonctions ne sont pas anodines et le sont encore moins en matière de violation de données. En effet, elles vont être mises à contribution dans le cadre de la gestion d'une telle violation.

1. Formation et sensibilisation du personnel

Il appartient au DPO de veiller à la mise en place d'un réel programme de formation destiné au personnel participant aux opérations de traitement incluant, entre autres, la prévention des violations de données à caractère personnel. Par ce biais, il pourra réduire le risque de telles violations, mais aussi sensibiliser le personnel à la nécessité légale de faire remonter toute information relative à une violation de données à caractère personnel. Il est crucial que chacun mette la sécurité au centre de son attention et appréhende les risques provoqués par des comportements inadéquats.

2. Mise en place d'un processus de remontée et de traitement de l'information

Cette formation/sensibilisation s'appuiera sur l'élaboration d'un processus de remontée et de traitement d'information vers le responsable du traitement/sous-traitant afin qu'il puisse remplir, le cas échéant, ses obligations de notification prescrites aux articles 33 et 34 du GDPR. Dans le cadre de sa fonction, le DPO devra conseiller le responsable de traitement/sous-traitant pour adopter un processus qui soit en adéquation avec le GDPR et lui permettre de pouvoir effectuer une analyse adéquate de toute violation de données à caractère personnel et de la nécessité de procéder à la notification requise dans les délais impartis. Ce processus est crucial et doit impliquer le DPO pour son versant juridique, mais également le conseiller en sécurité ou, à défaut, le responsable de l'IT qui devra développer les outils technologiques nécessaires à la mise en place dudit processus et apporter ses propres compétences.

3. Association à la gestion de la violation et contact avec l'Autorité de protection des données (APD)

Le troisième niveau d'intervention du DPO sera la gestion elle-même de la violation de données à caractère personnel. En effet, le DPO devra contrôler le respect des articles 33 et suivant du GDPR, qui concernent la notification de la violation. Son rôle sera, à notre sens, important pour conseiller le responsable de traitement/sous-traitant sur les mesures à prendre pour assurer le respect de ces deux articles. Il s'appuiera, pour ce faire, sur le processus de remontée et de traitement de l'information mentionné ci-dessus, mais également sur le conseiller en sécurité ou sur le responsable de l'IT. Le DPO deviendra également la personne de contact avec l'APD et la personne concernée ainsi que l'article 39 lui en donne la mission. Il devra donc maîtriser parfaitement le dossier, ce qui implique, à nouveau, un processus de remontée et de traitement de l'information efficace et fonctionnel.

Les étapes de la gestion des incidents

Avant tout, le processus de gestion des incidents de sécurité doit intégrer un principe d'anticipation de ce qu'il convient de faire pour détecter les incidents et y apporter une réponse adéquate et rapide : la vitesse de réaction permet souvent de limiter les impacts d'un incident, comme l'indisponibilité du système d'information avec des conséquences parfois lourdes sur les activités.

Le processus de gestion des incidents de sécurité[3] inclut habituellement les étapes suivantes.

1. Se préparer aux incidents

Cette première étape consiste d'abord à mettre en œuvre des mesures techniques et organisationnelles pour détecter les incidents de sécurité. Elle prévoit aussi d'élaborer des plans de réponse pour guider les actions et les décisions utiles en cas de survenance d'incident.

Les rôles, les responsabilités et les acteurs doivent ensuite être fixés afin de mettre rapidement en place l'équipe chargée de gérer un éventuel incident (Computer Security Incident Response Team – CSIRT). Le DPO, le responsable du traitement et le responsable de l'IT en font naturellement partie, tout comme des experts externes, chargés par exemple de mener une cyberenquête, qui consiste à établir un dossier juridiquement recevable pour d'éventuelles poursuites à venir.

Finalement, l'organisation veillera à établir un répertoire des actifs du système d'information, comme des données, des processus logiciels réalisant les traitements, ou des composants matériels. Un inventaire des traitements[4] est d'ailleurs imposé par le GDPR et il est judicieux de l'étendre à l'ensemble des actifs.

2. Détecter un incident

Deux sources principales signalent un incident de sécurité : les utilisateurs et les outils automatiques de détection.

Une fois détecté, l'incident doit être analysé en détail. Cette analyse porte au minimum sur la nature et l'étendue

[1] Une « violation de données à caractère personnel » est une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données. (art. 4, 12), du GDPR).

[2] Art. 39, 1., e) du GDPR.

[3] Cyber Security Coalition. (2018, 01 17). Media. Récupéré sur www.cybersecuritycoalition.be : www.cybersecuritycoalition.be/content/uploads/cybersecurity-incident-management-guide-FR.pdf.

[4] Art. 30 du GDPR.

des actifs impactés, et sur les circonstances techniques de l'incident, comme l'origine d'une attaque. L'incident et sa description seront consignés dans un registre *ad hoc*, tout comme les actions entreprises pour le traiter[5]. Notons que le GDPR n'impose pas de structure pour ce registre, mais une information complète contribue à une bonne gestion de l'incident.

Le cas échéant, une cyberenquête sera diligentée afin d'engager un éventuel recours auprès des auteurs à la source de l'incident.

Ensuite, le responsable du traitement notifiera l'incident à l'ADP s'il concerne une fuite de données à caractère personnel[6], pour autant qu'il existe un risque de conséquences négatives sur les personnes concernées.

Si le risque pour les personnes est jugé élevé, le responsable du traitement devra en informer les personnes concernées dans les meilleurs délais[7]. La communication devra être claire et accessible. Elle précisera la nature de la violation de données, une personne de contact (souvent le DPO), les conséquences possibles de l'incident et les mesures activées pour y répondre. Le responsable du traitement fournira aussi toute autre information utile pour atténuer les conséquences de la violation, comme conseiller de changer de mot de passe si des données d'identification ont été compromises.

Le DPO a pour mission d'informer et de guider le responsable du traitement dans ces démarches.

3. Traiter un incident

Le traitement de l'incident proprement dit recouvre un ensemble d'actions techniques pour limiter la portée et la propagation de l'incident. Le responsable de l'IT tentera d'isoler les éléments du système affectés par l'incident, avant d'éradiquer tout ce qui est associé à l'incident, comme des virus.

4. Reprendre les activités

L'objectif du responsable de l'IT consistera ici à revenir le plus rapidement possible au fonctionnement normal du système. Les tâches correspondantes consistent à remettre le système en bon ordre afin d'empêcher tout nouvel incident, et à restaurer les données dans le meilleur état possible à partir de copies de sauvegarde en cas de compromission.

5. Tirer les enseignements

La survenance d'un incident doit être l'occasion d'améliorer le processus de gestion d'incidents en analysant la manière dont ils ont été gérés, et en identifiant les lacunes et les améliorations possibles dans les réponses apportées.

Quelques conseils des professionnels[8]

Les professionnels insistent sur l'importance de formaliser les processus de gestion des incidents car, en la matière, la question n'est pas de savoir si un incident de sécurité risque de se produire, mais quand il va se produire.

S'il paraît évident que la priorité doit être mise sur les incidents de sécurité dont on redoute un impact sur la protection des données personnelles, il semble intéressant d'inclure dans le processus de traitement les questions et les demandes issues de l'extérieur de l'entreprise (clients, prospects et autres). En effet, plusieurs études[9] semblent démontrer que près d'un quart des problèmes sont détectés par ces « externes ». Il convient donc de rendre visible un point de contact auprès duquel ces personnes pourront déclarer les incidents ou poser leurs questions. À cet égard, de plus en plus d'organisations disposent sur leur site internet d'une page consacrée à la vie privée sur laquelle le visiteur peut trouver une adresse mail de contact. Le personnel peut quant à lui prendre contact avec le service support (help desk ou autre) ou avec le point de contact utilisé pour les externes.

Comme nous l'avons évoqué précédemment, les experts du terrain insistent sur l'importance de disposer d'un CSIRT qui sera en charge du suivi de l'enregistrement d'un incident à sa clôture.

Par ailleurs, il faut prendre conscience que peu d'organisations sont à même de détecter en temps réel la survenance d'un problème de sécurité. Dans ce contexte, la détection de « signaux faibles » (p. ex. un ralentissement inhabituel des applications ou du réseau) permet de résoudre certains problèmes et parfois même de déjouer des tentatives de hacking.

De plus, si l'entreprise veut pouvoir tirer des enseignements des incidents de sécurité internes, elle doit absolument faire en sorte que ceux-ci ne soient pas dissimulés mais soient relatés aux responsables. Est-il nécessaire de préciser que la personne concernée doit bénéficier d'une impunité sans laquelle le processus ne peut fonctionner ?

Enfin, suivant la gravité des faits, il convient parfois de mettre en œuvre des techniques de cyberenquête qui permettront de garder les traces d'effraction tout en maintenant leur caractère probant. À cet égard, il est essentiel de se référer à des spécialistes (Police et autres) qui seront à même de traiter la question selon les règles de l'art.

Toutefois, il paraît opportun de minimiser les risques en amont de l'incident en menant une réflexion sur la gouvernance des données et sur l'enregistrement et le traitement des données nécessaires à la conduite de la mission de l'entreprise. Comme dans bien d'autres domaines liés à la sécurité, les employés constituent ici un maillon essentiel qu'il faut impliquer par divers moyens tels que la sensibilisation et la formation.

Alain Ejzyn
Directeur du Certificat en management de la sécurité des systèmes d'information (ICHEC/UNamur)

Thierry Van den Berghe
Professeur à l'ICHEC Brussels Management School

Jean-Marc Van Gyseghem
Avocat au barreau de Bruxelles
Directeur de recherche au Crids
DPO d'AVOCATS.BE

[5] Art. 3 du GDPR.
[6] Art. 33 du GDPR.
[7] Art. 34 du GDPR.
[8] Cette partie a été rédigée avec l'aide de C. Cantillon (RTBF) et D. Grégoire (Forem).
[9] C. COOPER, « How data breaches are discovered », *CSO Online*, 2 février 2017.